HP StorageWorks Fabric OS 5.3.0c release notes

hp

®

i n v e n t

Version

5.3.0c

Effective date

November 2007

Description

Fabric OS 5.3.0c is a patch release that contains fixes since the release of Fabric OS 5.3.0b. There is no new device support added with this release for HP StorageWorks platforms.

Update recommendations

HP strongly recommends that users upgrade to Fabric OS 5.3.0c as soon as possible, particularly if your model is the Brocade 4Gb SAN Switch for HP c-Class BladeSystem (Brocade 4024) and you are running a version older than 5.3.0b.

Consider the following before upgrading:

- If upgrading from Fabric OS 5.1.x, install Fabric OS 5.3.0c before installing the latest port and intelligent blades in the 4/256 Director.
- If upgrading from Fabric OS 5.1.x with switches running 2.6.x in the fabric, upgrading to 5.3.0c is not supported unless 2.6.x switches are separated by a Router.

Supersedes

Fabric OS 5.3.0b released in November, 2007.

Supported product models

- HP StorageWorks 4/8 SAN Switch and 4/16 SAN Switch (Brocade 200E)
- HP StorageWorks 4/64 SAN Switch (Brocade 4900)
- HP StorageWorks 400 Multi-protocol Router (Brocade 7500)
- HP StorageWorks 16 Port 4Gb Blade (FC4–16)
- HP StorageWorks 32 Port 4Gb Blade (FC4–32)
- B-Series MP Router Blade (Brocade FR4–18i Blade)
- HP StorageWorks 4/48 SAN Director Blade (FC4–48)
- HP StorageWorks SAN Switch 2/8V (Brocade 3250)
- HP StorageWorks SAN Switch 2/16V (Brocade 3850)
- HP StorageWorks SAN Switch 2/32 (Brocade 3900)
- HP StorageWorks SAN Switch 4/32 (Brocade 4100)
- HP StorageWorks 4/32B SAN Switch (Brocade 5000)
- HP StorageWorks SAN Director 2/128 (Brocade 24000 Director)
- HP StorageWorks 4/256 SAN Director (Brocade 48000 Director)
- HP StorageWorks B-series iSCSI Director Blade (Brocade FC4-16IP)
- Brocade 4Gb SAN Switch for HP p-Class BladeSystem (Brocade 4012)
- Brocade 4Gb SAN Switch for HP c-Class BladeSystem (Brocade 4024)

Support for embedded switch models

The B-Series embedded switches have transitioned from supporting the Fabric OS 5.0.5 stream only, to operating with Fabric OS 5.2.1b and later. The B-Series embedded switch models include:

- Brocade 4Gb SAN Switch for HP p-Class BladeSystem (Brocade 4012)
- Brocade 4Gb SAN Switch for HP c-Class BladeSystem (Brocade 4024)

📝 NOTE:

The Fabric OS 5.0.5 stream remains active for the Core Switch 2/64 and for the SAN Director 2/128 in chassis modes 3 and 4.

Unsupported product models

- HP StorageWorks Core Switch 2/64, which operates with Fabric OS 5.0.x (Brocade 12000)
- HP StorageWorks SAN Switch 2/16, which operates with Fabric OS 3.2.x (Brocade 3800)
- HP StorageWorks MSA SAN Switch 2/8, which operates with Fabric OS 3.2.x (Brocade 3000)
- HP StorageWorks Multi-protocol (MP) Router, which operates with XPath OS 7.4.x (Brocade AP7420)

📝 IMPORTANT:

Any enhancements for the above models will be delivered in Fabric OS 3.2.x, Fabric OS 5.0.5x, and XPath OS 7.4.x sustaining releases.

Devices supported

See the *HP StorageWorks SAN design reference guide* for supported devices: http://www.hp.com/go/san.

Operating systems

See http://www.hp.com/go/san for a list of operating systems.

New features in Fabric OS 5.3.0

This section lists Fabric OS 5.3.0 added features and improvements:

📝 NOTE:

The Fabric OS 5.3.0c patch firmware contains the same features introduced in Fabric OS 5.3.0.

- IPv6 support for the management ports
- Firmware download enhancements:
  - Support for Secure Copy (SCP)
  - Support for passive FTP
- iSCSI Blade – FC4-16IP enhancements
  - Support for iSCSI re-direction
  - Support for CHAP binding
  - Support for LUN delete from a virtual target

- Access Gateway mode support on the HP StorageWorks 4/16 SAN Switch (not supported on the 4/8 SAN Switch)
- Access Gateway enhancements:
  - Web Tools support
  - Fabric Manager support
  - NPIV on F_ports
- Fibre Channel Routing enhancements
- IP Broadcast zone support
- IP over FC also via FCR
- IP Filter support (formerly MAC and Management port ACLs in Secure Fabric OS (SFOS))
- Support for FCS with base Fabric OS (formerly in SFOS)
- Support for multiple NTP servers
- Port mirroring for 4/32B switch
- Security Enhancements
  - Support for security Admin role
  - Support for account lock-out for admin role
  - Support for strong password policies preventing repeat or sequence characters
  - P-EAP/MS-CHAPv2 support for RADIUS
- FC-IP
  - Fast Write and Tape Pipelining are supported over secure tunnels (not supported by HP at time of release of these release notes)
  - Differentiated Services Code Point (DSCP) markings.
- New FC Fast Write feature
- New SNMP Features
  - SNMP AD/RBAC support
  - 3DES and AES privacy protocol support
  - FCIP MIB
  - IPv6 trap destination
  - IPv6 SNMP ACL entries.

Access Gateway support

Access Gateway is supported in the following HP products only:

- Brocade 4Gb SAN Switch for HP p-Class BladeSystem (Brocade 4012)
- Brocade 4Gb SAN Switch for HP c-Class BladeSystem (Brocade 4024)
- HP StorageWorks 4/16 SAN Switch (Brocade 200E)

IMPORTANT:

The HP StorageWorks 4/8 SAN Switch, although using the same hardware as the 4/16 SAN Switch, does not support Access Gateway. Also, Access Gateway mode is not supported with the Brocade 4Gb SAN Switch for HP p-Class BladeSystem (Brocade 4012) if any half-height BladeServers (BL3xp) are configured in the same sleeve within the p-Class enclosure. Please check http://www.hp.com for the latest updates.

Access Gateway was initially introduced with Fabric OS 5.2.1b. It allows a switch to operate in a special agmode that allows simplified connectivity between large numbers of servers and the SAN. Access Gateway leverages N_port ID virtualization (NPIV) to hide the complexity of the servers (both physical and virtual) attached to it while allowing easy SAN connectivity. The edge fabric switch provides all the fabric services while Access Gateway connects to the edge switch by what appears as a Host Bus Adapter (HBA) connection. This architecture allows the deployment of many additional servers without

requiring a domain and the associated fabric rebuild traffic that is prevalent when switches are powered on, or added, or removed from a fabric.

Refer to the *Brocade Access Gateway Administrator's Guide* available on http://www.hp.com/go/san for more information.

Access Gateway support in non-Brocade fabrics

In addition to being supported in Brocade fabrics, Access Gateway is supported for connectivity to the following:

- McDATA fabrics running EOS 09.00.xx with Brocade FOS 5.2.1b
- McDATA fabrics running EOS 09.02.xx or 09.03.xx with Brocade FOS 5.3.0, 5.3.0a, 5.3.0b or 5.3.0c
- Cisco fabrics running SAN-OS 3.0(2a) with Brocade FOS 5.2.1b
- Cisco fabrics running SAN-OS versions 3.1(2a), 3.1(3), 3.1(3a) with Brocade FOS 5.3.0, 5.3.0a, 5.3.0b or 5.3.0c

Dynamic Ports on Demand (DPOD)

> **IMPORTANT:**
>
> DPOD is an optional features supported in the following HP product only:
>
> - Brocade 4Gb SAN Switch for HP c-Class BladeSystem (Brocade 4024)
>
> Please check http://www.hp.com for the latest updates.

DPOD takes the expansion capability of fixed Ports on Demand (PODs) and adds the flexibility of connecting to any available port as long as a valid license is available. Previously, POD allowed only specific ports to be utilized. With DPOD, any physically available port can be made active as long as a valid license is available. This allows customers the flexibility of automatically changing port assignments where previously the port assignments were fixed and inflexible.

Reliability, Availability, Serviceability (RAS)

The RASLog is modified to support IPv6. RAS will also obsolete `traceftp` and `savecore` CLI and add its functionality to `supportsave` and `supportftp`.

Management

Fabric OS 5.3.0 added a new user role, the `secAdmin` or Security Administrator. This role maintains security administration including logging and auditing. The addition of the `secAdmin` role allows users to isolate security management from complete Administrator management.

Security

Secure Fabric OS is no longer sold as an option, but integrated into Fabric OS 5.3.0 and later.

> **IMPORTANT:**
>
> Fabric OS 5.3.0 is the last major release that is compatible with SFOS.

Fabric OS 5.3.0 integrated the following new features:

- FICON Cascading no longer requires SFOS
- MAC policies have now been replaced by IP filters, allowing configuration of acceptable IP addresses and ranges that may gain management access to the switch.
- Protected-Extensible Authentication Protocol (P-EAP with MSCHAP-v2) support for RAdmin DomainIUS.

- DH-CHAP now supported for authentication of HBAs and end-devices in addition to switches
- Additional password security options
- Lockout of Admin users that fail authorization.
- Flexible E_Port authentication settings, allowing better interoperability options for fabrics with varying levels of support. Certificate authentication is now optional.
- Auditing of authorization attempts.

Additional enhancements

Additional enhancements include:

- New optional FC Fast Write feature for the 400 MP Router (Brocade 7500) and B-Series MP Router Blade (FR4–18i) provides optimization and performance improvements for synchronous SCSI write operations.
- SAS re-direction provides simplified virtualization configuration.

New Web Tools features in Fabric OS 5.3.0

Web Tools updates include:

- Usability enhancements
    - Web-started GUI
    - Revamped Switch Explorer
    - Single-signed application
    - Common GUI components with new search and export capabilities
    - "Advanced" vs. "Basic" views in Switch and Port Admin modules
    - Progress bars, additional window handling improvements
- Access Gateway enhancements
    - Full configuration of Access Gateway parameters such as port mapping, Failover and Failback policies
    - Tabular display of port mapping, port settings, port status, and WWN of attached devices.
- iSCSI setup wizard for improved usability
- IPv6 support
- Support for Security Admin role, P-EAP protocol
- WTEZ Switch Setup enhancements
- Passive FCS support (enforcement but no configuration)
- IP Filtering
- FC Fast Write support

Prerequisites

Table 1 summarizes current Fabric OS firmware versions. However, HP recommends using the latest supported firmware release versions to get the greatest benefit from the SAN.

For a list of retired products, visit the HP web site http://www.hp.com.

Table 1 Current supported Fabric OS versions

Model	Earliest compatible version	Recommended version
HP StorageWorks 1 Gb Switch	2.6.2c	2.6.2d[1]
HP StorageWorks SAN Switch 2/8–EL, HPStorageWorks SAN Switch 2/16, MSA SAN Switch 2/8	3.2.1	3.2.1c
HP StorageWorks Core Switch 2/64	5.0.5	5.0.5e
HP StorageWorks SAN Switch 2/8V, HP StorageWorks SAN Switch 2/16V, HP StorageWorks SAN Switch 2/32, HP StorageWorks SAN Director 2/128	5.1.0d	5.3.0c
HP StorageWorks 4/64 SAN Switch	5.1.0d	5.3.0c
HP StorageWorks B-Series MP Router Blade, HP StorageWorks 400 MP Router	5.1.0d	5.3.0c
HP StorageWorks B-Series iSCSI Director Blade (Brocade FC4–16IP)	5.2.1b	5.3.0c
HP StorageWorks SAN Switch 4/32	5.1.0d	5.3.0c
HP StorageWorks 4/32B SAN Switch	5.2.1b	5.3.0c
HP StorageWorks MP Router	XPath OS 7.4.x	XPath OS 7.4.1e
Brocade 4Gb SAN Switch for HP p-Class BladeSystem, Brocade 4Gb SAN Switch for HP c-Class BladeSystem	5.0.5	5.3.0c
Fabric Manager	5.2.0a	5.3.0a

[1] Fabric OS 2.6.x can interoperate with Fabric OS 5.2.x or later via FC routing capability of the HP StorageWorks Multi-protocol (MP) Router. HP StorageWorks 400 MP Router, or HP StorageWorks B-Series MP Router Blade. Refer to the *Fabric OS 5.3.0c release notes* (this document) for additional interoperability information.

IMPORTANT:

The B-Series MP Router Blade (for use with the 4/256 Director only) must run Fabric OS 5.1.0d or later. Note that the Core Switch 2/64 does not support the B-Series MP Router Blade.

Firmware upgrade instructions

IMPORTANT:

HP strongly recommends that users upgrade to Fabric OS 5.3.0c as soon as possible (particularly if your model is the Brocade 4Gb SAN Switch for HP c-Class BladeSystem, Brocade 4024.

To access the latest Fabric OS 5.3.0c firmware, configuration files, and MIB files, go to the following HP web site: http://www.hp.com/go/san.

△ **CAUTION:**

Install port blades like the HP StorageWorks 4/48 SAN Director Blade (FC4–48) only after upgrading to Fabric OS 5.2.0a or later.

HP does not support directly upgrading from more than two previous releases. For example, upgrading from Fabric OS 5.1.x to 5.3.0c is supported, but upgrading from Fabric OS 5.0.x or a previous release directly to 5.3.0c is not.

Upgrading a switch from Fabric OS 5.0.x or a previous release to 5.3.0 requires a two-step process: first upgrade to Fabric OS 5.1.x or 5.2.x and then upgrade to 5.3.0c.

The following conditions must be met before upgrading to Fabric OS 5.3.0c:

- Device-based routing must not be in use, otherwise the upgrade will fail. You can use the `aptPolicy` command to verify the routing policy.
- Chassis configuration options 3 and 4 are no longer supported for the 4/256 SAN Director.
- Fabric OS 5.1.1 supports a maximum MTU value of 2284. However, Fabric OS 5.2.1x and 5.3.0x support an MTU value of up to 2348. Prior to downgrading the Fabric OS to 5.1.1 you must change the MTU size less than or equal to 2284.
  If the configuration of the target unit has an MTU value greater than 2284, the FCIP tunnels will not go online after firmware downgrade.

△ **CAUTION:**

If the 4/256 SAN Director integrates the FC4–48 Blade or any new software features in Fabric OS 5.2.0a, such as FCR trunking, you cannot downgrade below Fabric OS 5.2.0a. If you want to do so, you must (a) remove these features, (b) physically remove the Blade, and then (c) downgrade the firmware.

- For any other new software features or increased scalability limits supported by Fabric OS 5.3.0c, downgrade will be disruptive and require cold reboot.
- A Fabric OS 5.3.0c configuration file cannot be used on the same switch after the switch has been downgraded to firmware version 5.1.x or 5.2.x.
- When you downgrade to Fabric OS 5.0.x, you must also remove additional 5.1.x features and any installed B-Series MP Router blades.

Important notes

Table 2 provides information relevant to the release of Fabric OS 5.3.0c.

Table 2 Important release information

Topic	Description

`ipfilter` command	Starting with Fabric OS version 5.3.0, you can use the `ipfilter` command to block unauthorized Telnet access. The option to disable Telnet using the `configure` command is no longer available.
	Use the following command to create a policy to block Telnet access to any station:
	`ipfilter --create blockTelnet -type ipv4 ipfilter`
	`--addrule blockTelnet -sip any -dp 23 -proto tcp -act deny`
	`ipfilter -- activate blockTelnet`
	Use the following command to restore default policies for IPv4:
	`ipfilter --activate default_ipv4 --`
	See the *Fabric OS 5.3.0 command reference guide* for more information on the `ipfilter` command.

PKI certification	If you have purchased and installed the Secure Fabric OS option, go to the following web site for information on obtaining a PKI certificate: http://www.hp.com/storage/go/secureos.

FICON support	With release 5.2.0 and later, the Switch Connection Control high integrity requirement for cascading FICON is available in the standard base Fabric OS. End users can now deploy new cascade FICON Directors without purchasing a separate Secure Fabric OS license. To add a new FICON Director into existing cascaded configurations already running Secured Fabric OS, HP recommends that users continue to deploy Secure Fabric OS on the new FICON Director instead of migrating to FOS ACL configuration. **NOTE:** The FC4–48 port Blade is not supported to connect to System z environments via FICON channels or via FCP zLinux on System z. To attach the Director to the System z environment, use an FC4–16 or FC4–32 Fibre Channel port Blade.
Diagnostics backport test	Backport tests may be run only in the following configurations: • A pure SAN Director 2/128 (only CP2 and FC-16 blades) • A SAN Director 2/128 with no FC4–16 blades installed, using Option 5. Do not run backport tests in any configuration other than the two listed above; use the minicycle test instead.
Diagnostics spinsilk test	The following configurations will *pass* the spinsilk test: • A pure SAN Director 2/128 (only CP2 and FC-16 blades) • A pure 4/256 SAN Director, Option 5 • A pure 4/256 SAN Director, Option 5 (with FC4–16 blades) The following configurations will *fail* the spinsilk test; use the minicycle test instead: • A mixed SAN Director 2/128 (with either CP4 or FC4–16 blades) • A pure 4/256 SAN Director, Option 1 (a pure 4/256 SAN Director refers to a Director with CP4 and FC4–16 blades only).
HP StorageWorks 400 MP Router	Fans operate at the correct speed; that is, at maximum on bootup. However, this initial speed may trigger an error message that indicates that the speed is too high (`Above threshold`). Disregard this message.
4/256 SAN Director	• Before moving the slider UP on a Control Processor Blade that is being activated, observe that the amber LED is not ON for the active CP for at least 5 seconds and that all LEDs display off on the new inserted CP. • In a core-edge design, when a fully-populated 384–port 4/256 SAN Director (populated with eight FC4–48 blades) is an edge switch in a large SAN, it can experience high CPU utilization and may panic if it becomes a principal switch. HP recommends deploying a high port-count switch as both core and principal switch to reduce fabric stress and provide ease of management.

FC4–48 port Blade for the 4/256 SAN Director	• The HP StorageWorks 4/48 SAN Director Blade requires a minimum of Fabric OS 5.2.0a. Do not insert the FC4–48 Blade into the 4/256c chassis until the chassis is running Fabric OS 5.2.0a or later. After Fabric OS has been updated and an FC4–48 has been installed, the Fabric OS will not be able to be downgraded earlier than 5.2.0a until the FC4–48 is removed. • The FC4–48 Blade supports only core PID (fmt 1) in Secure Fabric OS. • NPIV is supported only in ports 0 to 15 of the FC4–48 Blade. • Regarding long distance buffer credits, the FC4–48 has 560 credits available for long distance. The FC4–32 Blade has 624 credits available for long distance. • Regarding port mirroring, the FC4–48 is restricted to one F-port mirroring allowed between shared areas for ports 16–47. Port mirroring on ports 0–15 behaves the same as the FC4–32 Blade. • The `configure` command gives only a maximum login per port setting. The command allows over 127, where ports for the FC4–48 Blade will honor that value as long as its share area values are 127 or less. • Before replacing an FC4–32 Blade with an FC4–48 Blade, restore ports 16–31 of the FC4–32 Blade, if these ports are used for port swapping. Failure to do so will fault the FC4–48 Blade. The only way to restore the original settings is to add the FC4–32 Blade back into the slot and port swap the ports back to the port's default setting. • FC4–48 ports should not belong to the zone or in an administrative domain in which FICON devices reside. • The FC4–48 Blade does not support loop. Private L_Ports will be shown on these ports in `switchshow`, but will not participate in the fabric. • The `porttest` and `spinfab` commands on any platform will not work on E_Ports connected to an FC4–48 port. • The FC4–48 Fibre Channel port Blade is not supported to connect to the System z environments via FICON channels or via FCP zLinux on System z. To use the 4/256 SAN Director to attach to the System z environment, use the FC4–16 or FC4–32 Fibre Channel port blades. • In a zoning configuration with members D and P, where P is greater than or equal to 256, remove these configurations before downgrading to an earlier firmware version (5.1.x or 5.0.x). Otherwise, the downgrade will not be HA compatible with earlier versions. • All zones involving the shared ports (domain, port or WWN) of an FC4-48 Blade would be treated as session based in "interopmode 2" fabric configuration.

FC4–16IP iSCSI Blade for the 4/256 SAN Director (continued)	• Do not insert the Blade until the system is running Fabric OS 5.2.1b or later.
	• iSCSI virtual target creation involves adding LUNs to the virtual targets. The user discovers the LUNs by executing the `fclunquery` command. Testing has revealed that some devices do not respond properly to the LUN query. The user will need to use tools from the array vendor to determine LUN information required for iSCSI target creation.
	• Any uppercase letters used for the CHAP user name will be transformed into lowercase.
	• Users may install up to four FC4–16IP iSCSI blades per 4/256 SAN Director chassis, or any combination of up to four blades (FC4–16IP and B-Series MP Router blades), not exceeding the individual Blade limit per chassis. Valid combinations include:
	  • Three FC4–16IP blades + one B-Series MP Router Blade
	  • Two FC4–16IP blades + two B-Series MP Router blades
	  • One FC4–16IP Blade + two B-Series MP Router blades
	  • Two FC4–16IP blades + one B-Series MP Router Blade

Firmware upgrade/ downgrade	• When upgrading from Fabric OS 5.1.0x to 5.2.0x or 5.3.0x, if two or more inter-fabric links (IFLs) connect to an edge fabric, one IFL will stay online and the other IFLs will go online and offline. This will cause a temporary traffic disruption going from multiple IFLs to one IFL and then back to multiple IFLs. This is due to the new front domain consolidation feature in Fabric OS 5.2.0, where the IFLs connected to the same edge share the same front domain. • When downgrading from Fabric OS 5.3.0x or 5.2.x, FC traffic will be disrupted if there is front domain consolidation prior to the downgrade, even in the case of a single IFL. • Upon firmware download the FC4–16IP Blade does not preserve disabled GE_Ports in disabled state. If you want to retain GE_Ports in a disabled state across firmware download, you must configure them as persistently disabled.
Fabric OS—CLI commands	• Obsolete commands include slotOff and slotOn; use slotPowerOff and slotPowerOn instead. The portLogPortShow command is also now obsolete. • This release does not support underscore (_) as part of the name for *dd* and *ddset* in the iscsicfg command. • When performing a configdownload, you may receive a message stating "configDownload not permitted." This indicates that an invalid parameter was passed to the switch. The invalid parameter could be from a switch security policy, such as the password policy, or the NTP server address. This causes a partial configuration to be downloaded onto the switch. For example, when an NTP server address is invalid, configdownload fails and all data processed prior to the NTP server address data had already been saved in the switchand cannot be backed out. To fix the problem, correct the invalid parameter and re-issue the configdownload command.
Distance mode	Distance setting is not persistent. After a configuration uploads and downloads, distance settings reset and the desired distance is shown as 0.
FC Routing	• If an HP StorageWorks MP Router is present in the backbone fabric, the command fcrDisable may take up to 8 minutes to complete. If the MP Router is replaced by a B-Series MP Router Blade (FR4-18i) or an HP StorageWorks 400 MP Router, the command completes immediately. • EX_Port trunking is not enabled by default. • FCR switch does not support an edge fabric with one McDATA switch set to 'never principal'. The EX_Port connected to that edge fabric will not come up. • FCR switch does not support edge fabrics that consist of McDATA switches with 'domain ID offset'. The EX_Port connected to that edge fabric may fail the RDI process and will not come up. EX_Ports come up disabled (failed to init in time) if attached to a Native mode switch running EOS 9.x that has non-default DID offset configured. • Device discovery may fail when an HBA uses the GA_NXT name server query to discover devices through an FCR switch since the query is mishandled by the FCR.
Security	Remove any password enforced expiration of admin or root accounts before downgrading firmware to 5.0.1 or earlier versions.
Diagnostics	• All offline diagnostics commands should be used only when the switch is disabled. • Installing new SFPs during POST may cause POST to fail. Install SFPs only when the switch is online or if the switch is powered off. • When you use the diagnostic commands systemVerification and diagSetBurnin, the switch or Blade faults when the burn-in error log is full. Clear the burn-in log before running systemVerification or diagSetBurnin. • If there ISLs reside on the switch that are not used for routing because they have higher link costs, disable the links before running spinfab.

HA	If there is an already segmented port and backbone devices are exported to an edge fabric, a build fabric/fabric reconfiguration can occur after running `haFailover`. Ensure that there no segmented port exist before upgrading firmware.
IPSec for B-Series MP Router Blade (FR4–18i)	- IPSec implementation details: - Pre-shared key - Main mode (IKE negotiation protocol) - Tunnel mode in Encapsulating Security Payload (ESP) - IPSec specific statistics not provided. - No NAT or IPV6 support - FastWrite and Tape Pipelining will not be supported in conjunction with secure tunnels. - Jumbo frames will not be supported on secure tunnels. - ICMP redirect is not supported for IPSec-enabled tunnels. - Only a single secure tunnel will be allowed on a port. Non-secure tunnels will not be allowed on the same port as secure tunnels. - Modify operations are not allowed on secure tunnels. To change the configuration of a secure tunnel, you must first delete the tunnel and then re-create it with the desired options. - Only a single route is supported on an interface with a secure tunnel. - An IPSec tunnel cannot be created using the same local IP address if ipperf is active and using the same local IP address (source IP address). - Unidirectional supported throughput is ~104Mbytes/sec and bidirectional supported throughput is ~90Mbytes/sec. - An IPSec tunnel takes longer to come online than a non-IPSec tunnel.
Fabric Merge	Do not try to merge fabrics with conflicting domain IDs over a VE_Port. Before merging two fabrics over FC-IP with VE_Ports at each end, HP recommends that all domain ID and zoning conflicts be resolved.
Scalability	- Support for Default Zoning policies has been added to Fabric OS 5.1.0. Typically, when you issue the `cfgDisable` command in a large fabric with thousands of devices, the name server indicates to all hosts that they can communicate with each other. To ensure that all devices in a fabric do not see each other during a `cfgDisable` operation, you can activate a Default Zone with policy set to `no access`. If Default zoning policies show enabled, all `cfgEnable/disable` commands and zoning changes must be run from a switch in the fabric running Fabric OS 5.1.0/5.2.0a. - In large fabrics with more than 1,000 ports, HP recommends that the MS Platform Database be disabled. The Platform DB must also be disabled before downgrading to earlier versions of Fabric OS. This can be done using the `msPLMgmtDeactivate` command.
FRU insertion	The `FW_FRU_INSERTED` message is displayed twice when a power supply FRU is inserted and powered on. There is no functional impact.
System boot	Not all Fabric OS services run when the prompt becomes available during boot up. Wait for all the services to come up before using the switch or performing zoning actions.
Performance Monitoring	If the user tries to save more than 512 monitors using the `perfCfgSave` command, some of the monitors may be lost.
Management — Proxy switches	If you using a Fabric OS 4.x switch as an API or SMI-S proxy to manage a 5.1.0 switch, you must be running Fabric OS 4.4.0d.

FCIP	• Frame drops observed on FCIP slow links:
	  • The frame drops occur when the FCIP tunnel bandwidth is set to 10 Base-T (10Mbps), E1 (1.048Mbps), or T1 (1.544Mbps).
	  • With E1 or T1, frames drop even without an impaired link.
	  • With 10 Base-T, frame drops may be observed when a low impairment is put to the link.
	• The `portperfshow` command indicated incorrect (smaller) bidirectional throughput on the FCIP tunnel when Fastwrite/Tape Pipelining is enabled.
	• Fastwrite/Tape Pipelining did not inform user when it failed due to multiple equal paths configured on 2 GbE ports.
	• Backup jobs initiated from the Symantec BackupExec application slowed noticeably after adding significant I/O traffic from regular hosts and targets to the FCIP tunnel. A port-based routing policy must be used for Tape devices.

Access Gateway vs Standard Switch Mode	When using the Blade server SAN switch in Access Gateway mode, most switch features are no longer applicable. These features include Admin Domains, Advanced Performance Monitoring, direct connection to SAN target devices, Fibre Channel Arbitrated Loop support, Fabric Manager, FICON, IP over FC, ISL Trunking, Extended Fabrics, Management Services, Name Services (SNS), port mirroring, Secure FOS, SMI-S, and Zoning. These switch features are available in the default switch mode of operation. Access Gateway mode is not supported in the p-class Blade system if there are two half-height servers in the same sleeve (Server Slot 1 and 9, 2 and 10, and so on). Two p-class half-height servers in the same sleeve require Fibre Channel Arbitrated Loop operation. The c-Class half-height Blade servers do not require Fibre Channel Arbitrated Loop and work fine with both access gateway mode and Standard Switch Mode.
Access Gateway Mode Port State	When a disabled port on a switch in Access Gateway mode is connected to a configured loop HBA, the port state alternates between Nosync and Insync. The `switchShow` command displays the state of the remote HBA port that is continuously attempting to reconnect to the disabled port. Access Gateway mode is not supported in the p-Class BladeSystem if there are two half-height servers (BL3xp) in the same sleeve (Server Slot 1 and 9, or 2 and 10, etc). That configuration requires Fibre Channel Arbitrated Loop operation, which conflicts with Access Gateway mode. There is no such restriction with c-Class, since no servers require Fibre Channel Arbitrated Loop. Access Gateway supports only FCP initiator connections on the F_Ports. Note that cascading Access Gateway devices or connecting FCP targets, loop devices, or FICON channel/control units on the F_Ports are not supported.
`portcfgdefault` command function change for the Brocade 4Gb SAN Switch for HP c-Class BladeSystem	Beginning with Fabric OS 5.2.1b, the `portcfgdefault` command now resets the configuration to HP factory default port settings.
Update to Brocade 4Gb SAN Switch for HP c-Class BladeSystem instructions.	After connecting to the Brocade 4Gb SAN Switch via the Onboard Administrator (OA) `connect` command, you will be in the switch CLI prompt. To return to the OA serial prompt: • Type **Exit** to log out of the switch. • Press **Shift-Ctrl-underscore** (escape sequence) to return to the OA prompt.

Zoning considerations with FC4–48 Blade	B-Series switches running pre-5.2.0 firmware do not accept zone databases with Domain, Port Index, references to ports higher than 255. Zoning in Fabric OS 5.2.0 and later, therefore, do not allow a Domain, Port Index entry for ports above 255 to be created unless all switches in the fabric are at Fabric OS 5.2.0 or later versions. Once such an entry has been put into the zone database, an attempt to connect a pre-Fabric OS 5.2.0 switch to the fabric results in that switch being segmented with a Zone Mismatch segmentation reason. Any zoning that is already in use can continue to be used. However, in Fabrics containing pre-Fabric OS 5.2.0 switches, if new devices are added on the upper 16 ports (ports 32-47) of the FC4-48 port Blade, then WWN zoning has to be used for those devices. If there is an existing Domain Port Index zone that connects to ports 32–47, HP recommends that you transform just that zone to WWN zoning. This would minimize the likelihood of rebuilding the entire fabric. Fabrics containing only Fabric OS 5.2.0 and later switches have no zoning limitation.

Update to *Brocade 4Gb SAN Switch for HP c-Class BladeSystem installation instructions*, part number 5697–5678	On page 2, please update the following step:
	
	7. At the command line, type:
	
	`c bay x`
	Where *x* is the I/O bay where the switch is installed.
	
	to
	
	7. At the command line, type:
	
	`connect interconnect x`
	Where *x* is the I/O bay where the switch is installed.

iSCSI	• Enterprise storage array targets may not show up consistently in the disk management window of an iSCSI initiator when the same LUNs are mapped to two different virtual targets (VTs). When the initiator logs in to the VTs, the targets keep disappearing from the disk management window. If the session to one of the VTs is disconnected, the remaining VT appears and stabilizes in the disk management window. • Under certain conditions, hosts on an IP network may not be able to issue a ping command to iSCSI gateway ports in another subnet. You can work around this problem by issuing a ping command from the iSCSI gateway port. The hosts will then be able to successfully issue ping commands to the iSCSI gateway port. • An IP network disconnection lasting five seconds or more may cause COPA failure on the disconnected PC, which in turn may cause a loss of connection to an enterprise storage array • If traffic is run from hosts to certain targets with severe impairment conditions in the IP network for hours at time, throughput to the targets will drop, and may take up to 10 minutes to recover after the impairment condition is removed. Note that this problem is highly intermittent, and is unlikely to be seen in a customer environment. We believe that this issue is the result of host/target interaction, and is not the result of action on the iSCSI gateway. • A Microsoft windows PC host was unable to discover enterprise storage array LUNs. The Microsoft iSCSI initiator is able to discover targets if the software is uninstalled and reinstalled without the MPIO option.
Broadcast Zones	In Fabric OS 5.3.0 and later, a zone with the name "broadcast" (case-sensitive) is a special zone for setting up recipients of broadcast packets. In Fabric OS versions earlier than 5.3.0, a zone named "broadcast" does not have special significance. Therefore, you must make sure that if a broadcast zone is configured, then the active and standby CPs use the same Fabric OS version. Otherwise an HA failover might change the zone configuration.

Faulty SFPs	External port with a faulty SFP will be disabled, then enabled once good SFP is inserted. However, port will still show as faulty even though it is healthy. To get the correct "healthy" indication, after enabling the port with the good SFP, remove and re-insert it and the port will then show as healthy.
FC Fast Write	Note the following important information when using FC Fast Write: • Only World Wide Name (WWN) zone (including normal zone and FC Fast Write zone) is supported on FC Fast Write enabled port. • Only single device loop port is supported. • NPIV (example Access Gateway) port is not supported. • FCR backbone devices are not supported. That is FC Fast Write should not be enabled on backbone devices. • FCR edge to edge support is limited by all the target devices on given edge fabric that host talks to should be connected to a 400 MP Router or B-Series MP Router Blade in FC Fast Write mode. FC Fast Write should not be enabled on ports when testing the remote mirror application. • When a very high volume of traffic is being sent by host, FC Fast Write IOs may time out and frame may be dropped. • Within the context of FC Fast Write, L_Port is not supported in Fabric OS 5.3.0.
Web Tools	When the regional language is set to anything other than English, Brazilian Portuguese, French, German, Italian, Japanese, Korean, Traditional Chinese, Simplified Chinese or Spanish, Web Tools may not finish loading when connecting to a switch running FOS 5.3.0, 5.3.0a or 5.3.0b. The Switch Explorer progress bar hangs while initializing switch details. This problem is overcome by changing the regional settings for the operating system to English and re-loading Web Tools.

Additional Fabric OS 5.3.0 enhancements

Additional Fabric OS 5.3.0 enhancements include:

- Provides new Fabric OS commands to rename an alias, a zone and a zone configuration. `Zone -copy` copies the zone object to a new zone object. `Zoneobjectrename` renames the zone object.
- Detects and handles a corrupted zone configuration [`under /etc/fabos/zone*`] gracefully instead of rebooting. The switch also logs the error in RASLog.
- Adds a new command that provides both the WWN and serial number of the switch. Added an `-sn` option to display the serial number. For example, `wwn -sn` will return both the world wide name and serial number data
- Provides additional information on a faulty port in Fabric Watch to aid in troubleshooting.
- Enables use of passive FTP to download firmware.
- Enables the customer to specify a quality password policy that prevents the selection of passwords with consecutive, identical characters.
- Uses multiple NTP servers with the `tsclockserver` command for redundancy. For example, if one site NTP server fails (DR scenario) there is a backup that can be reached by the switches.
- Logs a RASLog message when a 2.x switch joins the fabric.
- HA failover and user notification occurs on the 4/256 SAN Director when there is a failed Ethernet chip (Oscillator chip).

Additional Web Tools 5.3.0 enhancements

Additional Web Tools 5.3.0 enhancements include:

- Provides individual error counters for FC ports from Port admin.
- Provides SFP TX/RX power information in DB level from Port admin from Web Tools.
- Provides the Clear Counter feature to reset all counters.

- Provides ability to clear 400 MP Router or B-Series MP Router Blade GE port Error counters using `portStatsClear` CLI command.

Fabric OS 5.3.0 fixes

Table 3 lists defects closed in the Fabric OS 5.3.0 firmware release.

Table 3 Fabric OS 5.3.0 closed defects

Closed defect summary	Solution
4/256 Director running FICON with fsmode enabled & DLS on and port based route policy panics after upgrade from Fabric OS 5.0.x to 5.1.x or 5.2.0.	Fixed per Fabric OS 5.3.0
Kernel Ops error when counter is overrun during stress to fail test.	Fixed per Fabric OS 5.3.0
Exception error on 4/256 can occur when performing port mirroring causing reboot.	Fixed per Fabric OS 5.3.0
`Tstimezone` command doesn't show correct time and date if `configdownload` interface is used to update timezone.	Fixed per Fabric OS 5.3.0
After executing trunk disable/enable on all edge switches in large scalability fabric, a 2/128 E_port became stuck in Loopback mode.	Fixed per Fabric OS 5.3.0
Admin Domains enforcement on SID/DID not performed. `Portmirror` allowed addition of mirror port in Admin Domain3 when SID and DID were not port members.	Fixed per Fabric OS 5.3.0
New active CP got Oops and reboot during initialization after `hafailover` command issued.	Fixed per Fabric OS 5.3.0
After CP reboot, VE tunnel doesn't come up due to GE0 port on FR4-18i stuck in No_Sync state when using copper SFP's.	Fixed per Fabric OS 5.3.0
Switch doesn't generate RSCN following zoning changes using `cfgEnable` in interop mode, resulting in no PLOGI from hosts, and no target discovery.	Fixed per Fabric OS 5.3.0
When more than the supported number of Ex_Ports attached to same edge fabric with FCR switches, switch may panic causing continuous rebooting.	Fixed per Fabric OS 5.3.0
When more than the supported number of intelligent blades (FR4-18i, FC4-16IP, etc) configured in 4/256, powering up the 4th and 5th blades at the same time results in a failover.	Fixed per Fabric OS 5.3.0
In rare occurrence, FR4-18i Blade could become faulty after firmware download and `slotpoweron` followed by `slotpoweroff`.	Fixed per Fabric OS 5.3.0
Tape backup job failures occasionally observed in congested IO conditions due to tape pipelining not properly handling target recovery.	Fixed per Fabric OS 5.3.0
After changing FID & enabling FCR switch, all connected/active ports remain disabled.	Fixed per Fabric OS 5.3.0
If active CP fails over after FC4-16ip port Blade runs `slotpower` on, all the FC4-16ip iSCSI ports can get stuck at "No_Sync" while FC ports come online.	Fixed per Fabric OS 5.3.0
After an all switches disable on 4/256 with FC4-48 port blades, standby CP asserted and rebooted.	Fixed per Fabric OS 5.3.0
`HAfailover` during FCIP IO through IPSec enabled tunnel sometimes causes VE port to go down, then come back up.	Fixed per Fabric OS 5.3.0

User was able to configure isns client via `isnsccfg` to communicate with isns server through a port on FR4-18i, but this will not work (nor should it).	Fixed per Fabric OS 5.3.0
FICON traps sent with wrong "Enterprise" value resulting in trap being processed as a swFault.	Fixed per Fabric OS 5.3.0
In Web Tools customized port detail report, the report will be generated for all ports even if the user gives a particular port range as a filter.	Fixed per Fabric OS 5.3.0
On 2Gb/s platforms, switch panic can occur if unstable or faulty port generates excessive number of interrupts.	Fixed per Fabric OS 5.3.0
When rebooting the active CP from Root, the warning text that is displayed when rebooting from Admin to warn that rebooting the active CP will disrupt traffic, is not displayed.	Fixed per Fabric OS 5.3.0
In edge to backbone fabric configuration with target in backbone fabric and host in edge fabric, 400 MP Router neither accepted or aborted a PLOGI. Only happens when there are devices in the fabric for which the link is taken online/offline quickly within a short period of time.	Fixed per Fabric OS 5.3.0
4/64 SAN switch with 5.1.0d experienced HW/SW interlock that became stuck requiring port disable/enable to clear the condition. This issue was not reproducible.	Fixed per Fabric OS 5.3.0
Using API to access default zoning information could cause switch to panic due to invalid pointer.	Fixed per Fabric OS 5.3.0
With large zoneset (over 1200 zones) API library crashes as the zone library does memcpy that doesn't have terminating zero in the buffer.	Fixed per Fabric OS 5.3.0
Change made in 5.2.0 to limit the number of FDISCs per unit of time, caused timeouts of NPIV logins in some BladeServer configurations with VC-FC.	Fixed per Fabric OS 5.3.0.
When FOS version prior to 5.2.0 is upgraded to a later version and the fabric.ops.mode.pidFormat value was previously set to zero, the switch will continually reboot.	Fixed per Fabric OS 5.3.0
In extremely rare conditions when a particular timing window is hit at the same time an internal end to end monitor wraps its counter, the standby CP can get stuck in a reboot loop. The condition is that due to a race condition, a partial HA update arrives before a full update from the active CP, resulting in standby CP going into continuous restart cycle.	Fixed per Fabric OS 5.3.0
When MS request issued with WWN that didn't exist in the fabric, the MS Daemon panicked.	Fixed per Fabric OS 5.3.0
The 2/128 was forwarding PLOGI frames received with DID as broadcast format which was causing issues with other devices in the fabric.	Fixed in Fabric OS 5.3.0. No longer forwards these type of frames.
For platforms running 5.2.0 and above with domain, port zoning, there is a small window during which if a device sends it PLOGI very fast, and before the nameserver information has been fully propagated, the PLOGI may be dropped.	Fixed per Fabric OS 5.3.0
CLI `systemverification` command incorrectly reports false positive failure on FC4-16IP Blade. This diagnostic command is not typically run by a customer.	Fixed per Fabric OS 5.3.0
"Stats" menu option doesn't work when executing `minicycle` command.	Fixed per Fabric OS 5.3.0

Process login drop due to devices in different edge fabrics with same node WWN. Applies to 4/256 with FCR-18i Blade, and 400 MP Router. Routers may not forward the `Nameserver` request to proper domain, resulting in request timeout & retries every 2 seconds.	Fixed per Fabric OS 5.3.0
In a FICON environment a Switch panic (in the Management Server daemon) could be seen if the switch receives one of three FICON specific frames (FICON GCAP, RLIR, RNID) and the fabric goes "unstable" (fabric being rebuilt such as when one of the switches in the fabric is powered off) before a response is sent.	Fixed per Fabric OS 5.3.0
Traffic can't be routed into backbone fabric from EX_Port on 400 MP Router with domain ID 7 or 12 and from FR4-18i Blade in 4/256 with various domain ID's.	Fixed per Fabric OS 5.3.0
Rapidly issuing repeated `supportsave` commands can cause switch panic due to out of memory condition.	Fixed per Fabric OS 5.3.0
When interop mode set to 1, "Disable NodeName Zone Checking" parameter also changes from 0 to 1, but returns to 0 after switch reboot.	Fixed per Fabric OS 5.3.0
Due to race condition in `RNID` command from FICON channels, FICON CUP daemon crashes and switch panics after switch comes up then it starts processing the `RNID` command. Problem affects FICON environment for Fabric OS 5.1 and later.	Fixed per Fabric OS 5.3.0
Web Tools error message provided when fmsmode setting fails is not clear.	Fixed per Fabric OS 5.3.0
Web Tools is missing "Invalid CRCS" under Fabric Watch end to end class pull down menu, due to missing "CRC Error" option.	Fixed per Fabric OS 5.3.0
GUI component size squeezed due to lack of proper refresh after resizing.	Fixed per Fabric OS 5.3.0
Errlog (raslog) messages not available for diagnosing DHCP problems.	Fixed per Fabric OS 5.3.0
Web Tools allows (switch,port) members to be added as member of a zone in interop mode, but this won't actually be created successfully.	Fixed in Fabric OS 5.3.0 by blocking addition of D,P members & D,P zoning when in interop mode.
Some switches are segmented with reason alias ID overlap when selected switches in fabric configured to use Alias Server due to lack of Alias Server support in Fabric OS 5.2.0.	Fixed per Fabric OS 5.3.0
On Solaris, when switch already in marginal state and another marginal event occurs, Events list in Call Home email not getting updated with exact reason for the alert.	Fixed per Fabric OS 5.3.0
FCIP error message not correct while editing/adding the subnet mask of an IP address that conflicts with the existing IP addresses.	Fixed per Fabric OS 5.3.0
EZManager doesn't differentiate ports as storage and hosts if no devices/hosts connections made.	Fixed per Fabric OS 5.3.0
During stress testing with large number of sent error frames leading to generation of very big core file, and watchdog timer timeout.	Fixed per Fabric OS 5.3.0
Enc out counter increases on unused ports on 2Gb platforms after HAreboot or firmware download.	Fixed per Fabric OS 5.3.0
Web Tools is not displaying "logged in" Radius account information.	Fixed per Fabric OS 5.3.0
Units for temperature, Rx and Tx power are not shown on SFP tab in Web Tools.	Fixed per Fabric OS 5.3.0
Web Tools doesn't display units of **Total Bandwidth** and **Bandwidth Demand** in **Fabric Topology** Window.	Fixed per Fabric OS 5.3.0

Web Tools incorrectly returns "Directory change failed" error message rather than "file path provided is not valid" error message when `config upload` fails due to invalid file path.	Fixed per Fabric OS 5.3.0
Modifying port speed and trunking on FC4-48 ports from Web Tools, followed by `HAfailover`, and then trying to re-launch, **Port Admin** window on those same ports fails to reload Web Tools window.	Fixed per Fabric OS 5.3.0
F_Port route cleanup doesn't happen correctly when NPIV is used on switch in Access Gateway mode.	Fixed per Fabric OS 5.3.0
EZSwitch Setup device display is overlapped in Display Connection window when window size not maximized.	Fixed per Fabric OS 5.3.0
`Portstatsclear` help page description of behavior on 2Gb and 4Gb platforms is ambiguous.	Fixed per Fabric OS 5.3.0
FR4-18i tracedump files contain many BP error messages and one empty file, potentially leading to incomplete support files.	Fixed per Fabric OS 5.3.0
During stress testing when rebooting all core switches in a loop, E-ports may get stuck in "Mod_Val" mode.	Fixed per Fabric OS 5.3.0
Error messages are generated when applying iSCSI easycreate operation from Web Tools on unreachable FC Targets. No error messages if LUN information is not retrievable from an FC Target. Errors are only displayed when applying the operation.	Fixed per Fabric OS 5.3.0
If Dynamic Load Sharing (DLS) or In-Order Delivery is disabled, it can't be enabled from Web Tools. However, it can be set/reset via CLI.	Fixed per Fabric OS 5.3.0
Web Tools event filtering uses a time range of 0-11 rather than 1-12. In Web Tools Fabric Events and Events window, on invoking filter button and filtering based on "from" time or "to" time, on providing a time greater than 12 (e.g. 12:30 PM) will result in an error stating that time should be in range of 0-11.	Fixed per Fabric OS 5.3.0
Additional Port Info column in FC Ports tab in Web Tools shows "None (FMS Mode)" instead of "Disabled (FMS Mode)."	Fixed per Fabric OS 5.3.0
FR4-18i blades rebooted during firmware commit process per `firmwaredownloadstatus` output. Process does recover.	Fixed per Fabric OS 5.3.0
With EZSwitchSetup, fixed zone can't be configured with all ports designated as storage or hosts. This is correct behavior, but the message displayed doesn't describe how to correct the misconfiguration should the user attempt to configure in that manner.	Fixed per Fabric OS 5.3.0
Error messages occur during IPsec FCIP IO.	Fixed per Fabric OS 5.3.0
Incorrect information returned during Request Node Identification Data (RNID) registration.	Fixed per Fabric OS 5.3.0
User sees wrong port type after port swap on issuing `fwsamshow` from CLI, due to port type getting swapped in the SAM Report.	Fixed per Fabric OS 5.3.0
Due to current handling of invalid zone type during zone enforcement after failover, Name Server daemon (nsd) panic results in CP fault after `firmwaredownload`.	Fixed per Fabric OS 5.3.0
Unable to view policy details in the absence of IPSEC license from "Show IP Security policies".	Fixed per Fabric OS 5.3.0
After changing an expired password and selecting another Admin Domain during the same session, the password expiration message and password prompt are displayed again. Currently have to exit session and re-login after changing an expired password to avoid this issue.	Fixed per Fabric OS 5.3.0

Error messages from ACL configuration through SMI are too generic and don't contain sufficient information to debug the problem.	Fixed per Fabric OS 5.3.0
Portstats: Selecting the "Show delta" radio button and clicking on the clear counter button, doesn't clear the counters. It changes the values to negative. Clicking the clear counter button again will reset counter to zero.	Fixed per Fabric OS 5.3.0
May see FFDC warning messages when manually changing switch IP address in DHCP network.	Fixed per Fabric OS 5.3.0
Able to establish API session to Admin Domain 255 using "user" login which has Admin Domain membership only to Admin Domain 0, which is not allowed from CLI, resulting in error. Users of SMI and Web Tools won't observe error because all operations performed via Admin role user.	Fixed per Fabric OS 5.3.0
Web Tools currently not consistent with CLI on configuring long distance for ports if current Admin Domain owns them but not `switchmembership`. Port long distance settings are read-only for owned ports on non-owned switches in Web Tools Extended Fabric tab, but editable for owned ports in Web Tools port configuration wizard.	Fixed per Fabric OS 5.3.0
SNMP traps repeatedly sent from the switch every 2 seconds when port taken out of a fault state implicitly by removing cable or module. Caused by too many port offline SCNs being sent out during port fault and recover when there is laser fault.	Fixed per Fabric OS 5.3.0
Firmware downgrade to Fabric OS 5.1 or earlier is blocked even after ports 256 – 384 are removed from DCC policy created using [*] option. Currently have to delete DCC policy to avoid this.	Fixed per Fabric OS 5.3.0
Admin user account with permissions to only Admin Domain 255 can create Admin Domains, but only Admin user accounts with permissions for all Admin Domains should be able to do this.	Fixed per Fabric OS 5.3.0
Confirmation dialog doesn't appear when name server table closed by clicking the "X" button. User experiences unexpected close when clicking "X" button.	Fixed per Fabric OS 5.3.0
Detailed view of any device doesn't refresh properly when Auto refresh option is selected & user resizes/scrolls the window.	Fixed per Fabric OS 5.3.0
Role name, and sometimes user name, missing from error message when user exits from a Telnet session.	Fixed per Fabric OS 5.3.0
The 2/16v switch produces ARB(vc) fill words instead of idles which could cause failures with certain long distance devices when running Fabric OS 5.2 with the following port configuration: —`portcfglongdistance` <*port*> LS 1 50 —`portcfgislmode` <*port*> 1	Fixed per Fabric OS 5.3.0
Web Tools not correctly reflecting physical switch state of a persistently disabled switch when the switch is fastbooted. LEDs are shown unlit instead of slowly blinking yellow.	Fixed per Fabric OS 5.3.0
No event is generated when the IP address of a switch is changed, so user can't determine IP address of the switch was changed by issuing the command `errdump` or `errshow` because IP address change event was not registered.	Fixed per Fabric OS 5.3.0
Several issues observed in ZoneAdmin and in Admin Domain when switch is configured in PID format 2, including being unable to see ports 16-32.	Fixed per Fabric OS 5.3.0

During stress testing, a significant delay in traffic coming back from a Fibre Channel Router (FCR) failure in fully redundant SAN configuration was seen, as traffic temporarily stopped before taking redundant path after rebooting one of the FCRs in dual back bone fabric.	Fixed per Fabric OS 5.3.0
During stress testing, switch may report fabric busy following issuance of a long string of operations repeatedly.	Fixed per Fabric OS 5.3.0
When using interactive mode to execute `pathinfo`, but with an invalid source port value, there is no error message.	Fixed per Fabric OS 5.3.0
After receiving login reject on FC4-16IP, subsequent login attempts may fail intermittently under some conditions. This can be avoided by moving the session back to init state after rejecting a login.	Fixed per Fabric OS 5.3.0
During stress testing, FC4-16IP may run out of memory if continually running `slotpoweroff/on` on multiple FC4-16IP blades for long period.	Fixed per Fabric OS 5.3.0
In Secure FOS, Web Tools gets null pointer from java console rather than the modify dialog to modify description and/or status when trying to modify default admin and user accounts.	Fixed per Fabric OS 5.3.0 which now includes all Secure FOS functionality.
Collecting `supportsave` info on 4/256 could cause error message on active CP console log.	Fixed per Fabric OS 5.3.0
Host takes a long time to log in when disabled/unused GE-iSCSI ports have IP addresses configured to them. When host does a "SendTargets=All" those IP addresses will be in the list, but will be unreachable.	Fixed per Fabric OS 5.3.0
After changing Backbone FID, `switchshow` doesn't display LE port information for some EX or VEX ports. Ports function correctly, only the display is incorrect.	Fixed per Fabric OS 5.3.0
On FC4-16IP iSCSI Blade, console log for iSNS reports the management port as slot/port 0/0.	Fixed per Fabric OS 5.3.0
With multiple FC4-16IP blades in multiple 4/256 directors in the fabric and ISNSC enabled, iSNS error message is logged on only one switch, but should be logged on all switches in the fabric.	Fixed per Fabric OS 5.3.0
May not see the targets after successful iSCSI login with FC4-16IP using AIX if immediate data is enabled.	Fixed per Fabric OS 5.3.0
LE ports not up after trunk disable/enable as evidenced by EX_Port not coming online.	Fixed per Fabric OS 5.3.0
`Switchshow` shows EX_Port left disabled after it's enabled due to setting VC Credits failure. In addition, when EX_Port trunk master is unplugged, non-trunk master ports are disabled.	Fixed per Fabric OS 5.3.0
Execquery Brocade_`SwitchFcPortRateStats` is not returning correct Instances. When Admin Domain's are created on the switch side without stopping the SMI-A, it always returns Instances with respect to Admin Domain0.	Fixed per Fabric OS 5.3.0
Sometimes when trying to add/modify Admin Domain list for multiple user accounts simultaneously, Admin Domain list for user accounts changes.	Fixed per Fabric OS 5.3.0
Port detail report shows incorrect values for iSCSI ports with FC4-16IP Blade.	Fixed per Fabric OS 5.3.0
`swFCPortOpStatus` of `swFCPortScn` is not reported correctly.	Fixed per Fabric OS 5.3.0
Excessive logins cause out-of-memory (OOM) panic while switching between user roles and executing `Configshow` command.	Fixed per Fabric OS 5.3.0

Vulnerabilities reported about open SSL VU#386964 & VU#547300. For VU#547300:OpenSSL SSL_get_shared_ciphers() vulnerable to buffer overflow. For VU#386964:OpenSSL SSLv2 client code fails to properly check for NULL.	Fixed per Fabric OS 5.3.0
Denial-of-Service condition affecting X.509 certificates verification (NISCC #729618) due to SSL vulnerability in OpenSSL. FOS 5.3.0 includes new version of OpenSSL that resolves this.	Fixed per Fabric OS 5.3.0
Incorrect time in Web Tools Switch Health report.	Fixed per Fabric OS 5.3.0
Incorrect F_Port behavior when RX side of the cable is disconnected, while the TX side is still inserted.	Fixed per Fabric OS 5.3.0
Installation of PKI certificate is delayed on any switch on which installation is attempted due to timing of the startup function.	Fixed per Fabric OS 5.3.0
The last character of config uploaded Banner (via "bannerset" CLI command) will disappear when performing a `configupload` followed by `configdownload`.	Fixed per Fabric OS 5.3.0
When connected to i10k Director in open mode, an RSCN received from the i10k was not immediately forwarded.	Fixed per Fabric OS 5.3.0
When upgrading 4/256 to Fabric OS 5.2.0b from 5.2.0a, both ISL trunk connections to an edge switch connected to FC4-16IP were lost. Found in test lab and due to "lab mode" setting, not accessible to customers.	Fixed per Fabric OS 5.3.0
Counter Address_err counting inappropriate data.	Fixed per Fabric OS 5.3.0
When assigning IP address to a GE port with no cable connection, the FC4-16IP Blade incorrectly reports back to iSCSI initiator that port is valid.	Fixed per Fabric OS 5.3.0
The 4/8 and 4/16 SAN Switches would display "Fan x is not faulty" messages on boot up after upgrade to Fabric OS 5.2.0x, even though fans were ok.	Fixed per Fabric OS 5.3.0
Disconnecting Rx end of cable on an L_port and leaving the Tx end unchanged results in unexpected behavior.	Fixed per Fabric OS 5.3.0
Access Gateway should handle an IPv6 address in a GMAL payload IP address in "ag – show" truncated to 16 characters (size of IPv4 address) depending on size of IP address string for edge switch to which N_Port attached.	Fixed per Fabric OS 5.3.0
`Switchdisable` and `switchenable` on switch that directly connects to storage will cause the storage to see GLIEN reject error message.	Fixed per Fabric OS 5.3.0
F_Port count is incorrect in `agshow` on the 4/32 SAN switch.	Fixed per Fabric OS 5.3.0
In CLI, iscsicfg –show/delete ddset –n xxx complains "requested object doesn't exist" even though it does exist, due to DD/DDSETs received from Microsoft iSNS server being in uppercase.	Fixed per Fabric OS 5.3.0

During iSCSI 1024 session stress testing, one port lost multiple sessions. Even though switchshow –iscsi showed less than 64 sessions, iSCSI initiator wasn't able to log in to the target (out of resources error).	Fixed per Fabric OS 5.3.0
Incorrect GID_FT response from NameServer. NameServer assumes device's FC4 type is FCP when GID_FT request is sent to the switch asking for PIDs of type FCP. PID of the sending device is incorrectly included in the reply list.	Fixed per Fabric OS 5.3.0
Unable to merge an upgraded switch with a 4/256 with FC4-48 Blade when using domain/port zoning of the upper 32 ports of the Blade. When creating D,P zoning definition using these upper 32 ports on FC4-48 connected to another switch running 5.1.0, the two switches correctly segment due to zoning conflict. After upgrading to 5.2.0, switches remain segmented, but segmentation should be removed.	Fixed per Fabric OS 5.3.0

Fabric OS 5.3.0a fixes

Table 4 lists defects closed in the Fabric OS 5.3.0a firmware release.

Table 4 Fabric OS 5.3.0a closed defects

Closed defect summary	Solution
Iswitchd panic occurred during data migration with DMM when invalid frame issued to the switch.	Fixed per Fabric OS 5.3.0a.
Diag failure caused FA4-18 to report a fault after continuously running CP failover test.	Fixed per Fabric OS 5.3.0a.
Panic occurred on SAN Director 2/128 when running MS commands GPT/GPPN/GPS/GAPNL continuously.	Fixed per Fabric OS 5.3.0a.
When the 4/64 SAN Switch is constantly rebooted, the Name server crashed in rare conditions.	Fixed per Fabric OS 5.3.0a.
4/32B SAN Switch running 5.3.0 rejected GID_Ft command from an HBA with "FC4-type not registered" error. HBA sees no devices.	Fixed in Fabric OS 5.3.0a by implementing a more robust zone name check to avoid confusing frame redirection zones with regular zone names.
In isolated cases, degraded performance can occur with the Brocade 4Gb SAN Switch for HP c-Class BladeSystem when internal ports are operated at 4Gb/sec.	Fabric OS 5.3.0a optimizes certain settings in the switch to address this issue.
Unable to configure FCIP tunnels using Web Tools in FOS 5.3.0.	FCIP wizard and stand-alone tab support added for near end tunnel configuration with Fabric OS 5.3.0a.
In frame redirect mode, GA_NXT query from initiator returns VI PID and PWWN instead of host PWWN.	Fixed per Fabric OS 5.3.0a.
scpd can crash on rare occasions due to memory leak in NS API/library during NS queries.	Fixed per Fabric OS 5.3.0a.
In Open mode, when F-Ports are connected to ports 16-47 on the FC4-48 Blade with WWN zoning, the Zone enforcement shows as SESSION BASED and the portcamshow command displays misleading information.	Fixed per Fabric OS 5.3.0a.
In frame redirect mode, GPN_NN query returns VI PWWN and PID instead of initiator PWWN and PID.	Fixed per Fabric OS 5.3.0a.

Fabric OS 5.3.0b fixes

Table 5 lists defects closed in the Fabric OS 5.3.0b firmware release.

Table 5 Fabric OS 5.3.0b closed defects

Closed defect summary	Solution
With FC Tape Pipelining enabled on a 400 MP Router/MP Router Blade FCIP connection, data written to tape using a block size of greater than 128 KB will not be readable by some applications, causing backup to be unreadable.	Backup application could be configured to use less than 128 KB block size to avoid the problem, but this is now fixed in 5.3.0b.
In rare cases, CRC errors can occur on Brocade 4Gb SAN Switch for HP c-Class BladeSystem internal ports when operating at 4Gb/s.	Fabric OS 5.3.0b addresses this issue.

When `supportsave` is run in a continuous loop, certain types of files are not detected which periodically generates the message:
`SupportSave completed sh:  /tmp/support-`
`Save_files/CONSOLE0:  No such file or directory.`
File name can vary.
	Fixed per Fabric OS 5.3.0b.

When the SFP/XFP power and voltage readings are above or below the range, an excessive number of alert messages were reported.	Fixed per Fabric OS 5.3.0b.
Third-party application will not work with the 400 MP Router Fast Write application (sends FCP_RSP without sequence initiative).	Fixed per Fabric OS 5.3.0b.
On the B-Series MP Router Blade or 400 MP Router, the proxy PID is improperly converted to 000000 for an ACC to a REC extended link request when an EX_Port is configured for interop mode. As a result, Tape backup may not work with devices in McDATA edge fabrics across the Router due to an improper response to a REC extended link request to a tape device.	Fixed per Fabric OS 5.3.0b.

Fabric OS 5.3.0c fixes

Table 6 lists defects closed in the Fabric OS 5.3.0c firmware release.

Table 6 Fabric OS 5.3.0c closed defects

Closed defect summary	Solution
I/O Ops failure due to incorrect CUP Port PDCM bit for port 256 after firmwareupgrade from FOS v5.1.x to FOSv5.2.x/5.3.x in FICON environment.	Fixed per Fabric OS 5.3.0c.
With McDATA edge switches in the fabric, 400 MP Router or FR4-18i router port receives periodic RRQ & ABTS frames due to the McDATA switch sending unsupported CT command. Routers don't respond, which causes McDATA switch to retry indefinitely.	Fixed per Fabric OS 5.3.0c to reject the unsupported `CT` command.
After `switchdisable` & `switchenable`, all 400 MP Routers or FR4-18i routers, proxydevices and nameserver entries no longer match what was previously recorded. "fcrrproxydevshow -a" shows 0 devices and translate domains are missing from the edge fabric. This is due to a timing issue while in open fabric interop mode with i10k switch when 2nd IFL is connected to the same switch in the fabric as the 1st IFL, and 1st IFL is fully up.	Fixed per Fabric OS 5.3.0c.
Hosts lose paths to targets due to FCR daemon failing to send GA_NXT response from 400 MP Router to host connecting to McDATA switch in open fabric mode. Caused by incorrect domain offset in its address translation.	Fixed per Fabric OS 5.3.0c.

When FRU in a 4/256 Director is inserted/removed a `fruHistoryTrap` should be generated, but is not.	Fixed in Fabric OS 5.3.0c. Note that `fruStatusChangeTrap` will not be generated with FRU `insert/remove`.
After upgrading switches to FOS 5.3.0, the Web Tools GUI bar showing the "Initializing Switch Details" will get stuck at 93% if the client's regional and language settings are set to some non-US languages such as Dutch, Russian, and Greek. English, French, German, Italian, Spanish, Portuguese, Simplified Chinese, Traditional Chinese, Japanese and Korean work fine.	Fixed per Fabric OS 5.3.0c.
A PLOGI received by 400 MP Router or FR4-18i prior to address translation table being programmed may not get the correct domain name offset while operating in the open fabric mode, leading to inability to boot over FCR connection for host that doesn't retry PLOGI.	Fixed per Fabric OS 5.3.0c.
Web Tools shows Ethernet speed at 0, even though it's operating at correct speed, due to underlying MAPS returning speed type rather than proper speed.	Fixed per Fabric OS 5.3.0c.